Wat is de relatie tussen security management en fact finding? Om deze vraag te kunnen beantwoorden, moet eerst duidelijk worden wat wij onder beide begrippen verstaan. Maar het één heeft baat bij het ander.

tekst Piet van Gelder en Bregje De Lanoy-Walenkamp

De voor- en achterkant van security

We beginnen met een schets van wat wij onder security management verstaan.

INSCHATTEN EN ANTICIPEREN OP WAAR HET MIS KAN GAAN

Bij security management staan de continuïteit van bedrijfsprocessen en de integriteit (imago) van een organisatie centraal. Insteek daarbij is dat incidenten worden voorkomen en - als ze zich toch voordoen - worden beheerst zodat eventuele schade/schande wordt beperkt. Neem bijvoorbeeld de toegangscontrole tot het bedrijfsterrein of bedrijfspand: hoe kan een aanval worden voorkomen? En hoe kan een aanval, als die toch plaatsvindt, in een zo vroeg mogelijk stadium worden gedetecteerd?
Security management gaat ook over het zodanig inrichten van bedrijfsprocessen, dat wordt voorkomen dat medewerkers of derden kans zien om bijvoorbeeld geld en/of goederen illegaal te bemachtigen. Ook hier geldt dat als men dit toch probeert: hoe kan dit dan zo snel mogelijk worden vastgesteld?

DRAAGVLAK VOOR INTEGRALE BENADERING ESSENTIEEL

Van belang bij security management is een integrale benadering in plaats van een incidentgestuurde benadering. Zo'n integrale benadering begint met een visie, gevolgd door beleid dat gericht is op de praktische uitvoering en implementatie van maatregelen en techniek. Top-down draagvlak creëren hiervoor is essentieel. Velen beschouwen dit soort maatregelen namelijk vooral als een kostenpost en een belemmering van de bedrijfsprocessen. Een medewerker die zich keer op keer op iedere verdieping in het bedrijfspand moet identificeren, ondervindt in de eerste plaats vooral hinder en is niet direct bezig met het grotere belang van het veiligheidsbeleid. Pas als ook deze medewerker het belang van de maatregelen inziet, kan het beleid effectief zijn.
Als het goed is, leidt een integrale aanpak tot het systematisch herkennen/beheersen van risico's en dreigingen.

RISICO'S IN KAART BRENGEN VERSUS DREIGINGEN BEPALEN

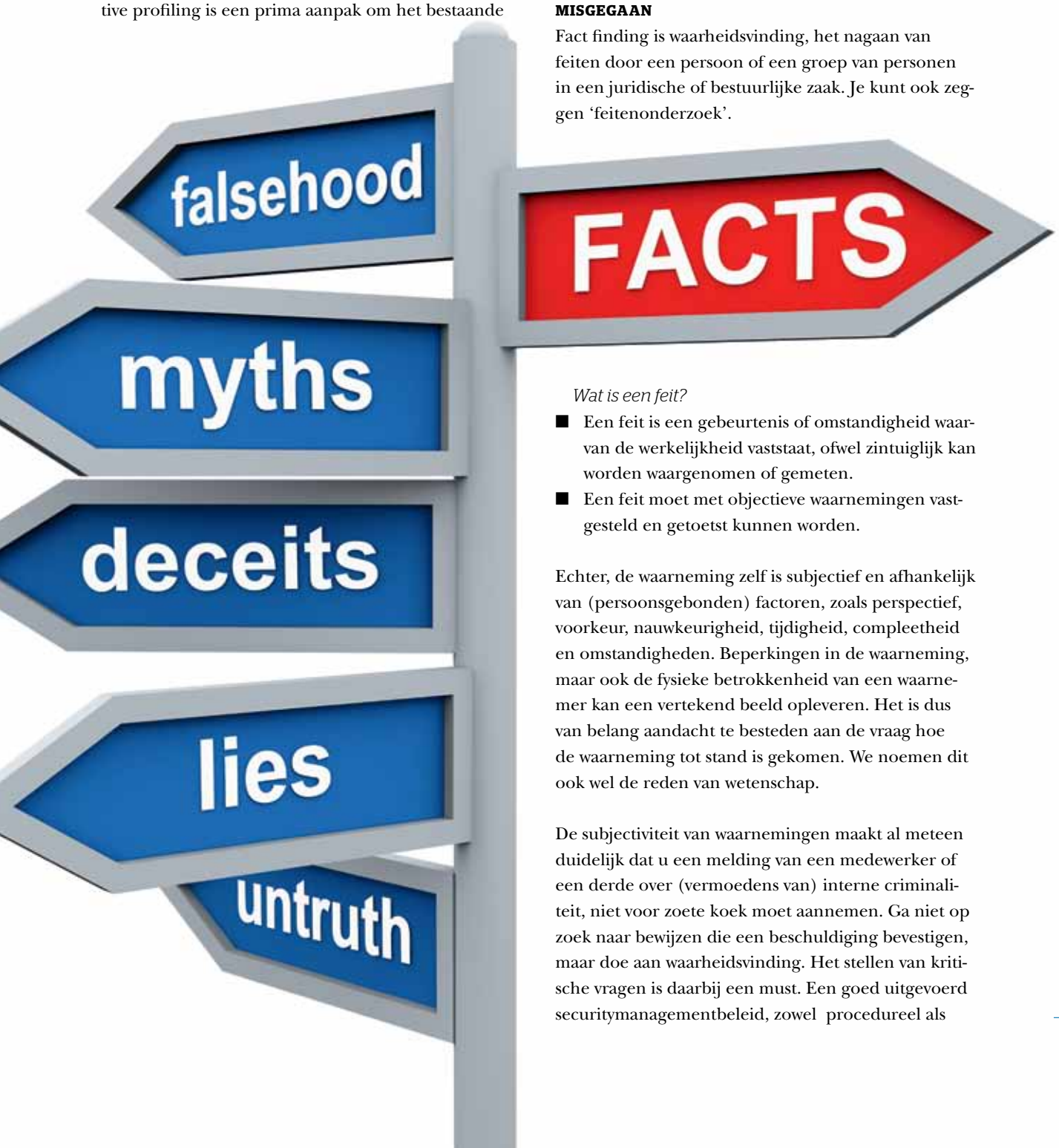
Van oudsher vormt de basis van security management een risicoanalyse. Hierbij worden de niet-handelsrisico's in kaart gebracht en vervolgens worden deze risico's geclassificeerd. Dit kan met behulp van de formule R = K x I, Risico is Kans maal Impact (of effect). Er zijn ook andere manieren, maar hier beperken we ons tot deze formule.
Een risico krijgt de classificatie hoog, middel of laag. Vervolgens wordt het beveiligingsniveau afgestemd op de risico's die zijn benoemd.
Tegenwoordig wordt meer en meer gebruik gemaakt van Risk Assesments. Daarbij worden meerdere personen en/of groepen uit de organisatie betrokken bij het in kaart brengen van de risico's. Een groot voordeel hiervan is dat er direct draagvlak wordt gecreëerd bij de betrokkenen voor te nemen beveiligingsmaatregelen.
Naast zo'n risicoanalyse wordt er ook steeds vaker - mede - gebruik gemaakt van predictive profiling. Bij

predictive profiling gaat het niet om risico's maar om dreigingen. Binnen de organisatie wordt in kaart gebracht welke werkwijzen kwaadwillenden zouden kunnen toepassen – de zogenaamde AMO's (AanvallersMethoden van Operatie) – om de organisatie aan te vallen. Voor deze AMO's worden indicatoren vastgesteld, waarna (security)medewerkers worden getraind in het herkennen van deze (verdachte-) indicatoren.
Vervolgens zijn zij in staat hier direct op te reageren volgens een afgesproken standaardprocedure. Predictive profiling is een prima aanpak om het bestaande beveiligingsniveau in de organisatie mee te toetsen, uit te breiden en naar een hoger niveau te tillen.
Dit geheel noemen we security management, dat zich dus vooral richt op de 'voorkant': 'het voorkomen van'. Security management stelt de organisatie als geheel in staat haar werk te doen, ondanks de aanwezige risico's en bedreigingen.

En wat is dan fact finding?

ONDERZOEKEN WAAR HET ONVERHOOPT TOCH IS MISGEGAAN

Fact finding is waarheidsvinding, het nagaan van feiten door een persoon of een groep van personen in een juridische of bestuurlijke zaak. Je kunt ook zeggen 'feitenonderzoek'.



Wat is een feit?

- Een feit is een gebeurtenis of omstandigheid waarvan de werkelijkheid vaststaat, ofwel zintuiglijk kan worden waargenomen of gemeten.
- Een feit moet met objectieve waarnemingen vastgesteld en getoetst kunnen worden.

Echter, de waarneming zelf is subjectief en afhankelijk van (persoonsgebonden) factoren, zoals perspectief, voorkeur, nauwkeurigheid, tijdigheid, compleetheid en omstandigheden. Beperkingen in de waarneming, maar ook de fysieke betrokkenheid van een waarnemer kan een vertekend beeld opleveren. Het is dus van belang aandacht te besteden aan de vraag hoe de waarneming tot stand is gekomen. We noemen dit ook wel de reden van wetenschap.

De subjectiviteit van waarnemingen maakt al meteen duidelijk dat u een melding van een medewerker of een derde over (vermoedens van) interne criminaliteit, niet voor zoete koek moet aannemen. Ga niet op zoek naar bewijzen die een beschuldiging bevestigen, maar doe aan waarheidsvinding. Het stellen van kritische vragen is daarbij een must. Een goed uitgevoerd securitymanagementbeleid, zowel procedureel als

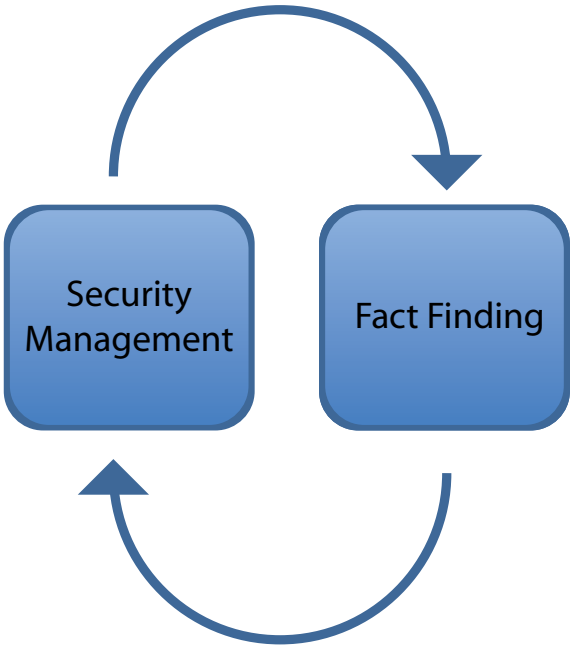
→

fysiek, kan hier enorm bij helpen en daar ligt naar onze mening ook de relatie. Hieronder zullen we dat nog verder benadrukken.

SECURITY MANAGEMENT ALS ONDERSTEUNING VAN FACT FINDING

Daar waar security management zich vooral richt op de 'voorkant', houdt fact finding zich bezig met de 'achterkant': pas als zich een incident heeft voorgedaan, zal daar onderzoek naar worden verricht. Neem het volgende voorbeeld:

Stel er is een laptop verdwenen van een medewerker op de linkervleugel van de 7e etage van het bedrijfspand. De vermissing zou hebben plaats gevonden op 12 november 2013 tussen 12.00 uur en 14.00 uur.
In het bedrijfspand is een goed toegangscontrolsysteem, ondersteund door een prima cctv-systeem. Het bedrijfspand bestaat uit 10 etages. Alle etages hebben en rechter- en een linkervleugel, die ieder afzonderlijk is gecompartimenteerd.
Voor de 7e tot en met de 10e etage geldt bovendien dat uitsluitend geautoriseerde medewerkers toegang hebben tot deze vleugels. Dat betekent dat als de badge van een medewerker niet is geautoriseerd, deze moet aanbellen om toegelaten te woren tot deze vleugels. Verder geldt er een draagplicht van de badges, die goed wordt nageleefd. Men spreekt elkaar erop aan als de badge niet gedragen wordt.



Voor het onderzoek naar de vermiste laptop kunt u dus met ondersteuning van het toegangscontrolesysteem en het cctv-systeem een analyse maken van de medewerkers die aanwezig zijn geweest in de desbetreffende vleugel toen de laptop zou zijn verdwenen. Dit leidt natuurlijk nog niet direct naar een betrokkene, maar het helpt wel mee. Als die maatregelen en systemen niet aanwezig zouden zijn, zou iedereen die in het pand was, verantwoordelijk kunnen zijn voor de vermissing. Sterker nog, als er helemaal geen toegangscontrole zou zijn, dan bestaat de hele buitenwereld uit mogelijke betrokkenen. De kans op een succesvol onderzoek wordt dan wel erg klein.

Mede dankzij een goed toegepast securitymanagementbeleid bestaat de kans dat met gezond verstand, een objectieve kijk op zaken (fact finding), en vasthoudendheid het onderzoek naar de vermiste laptop nu wel met succes wordt afgerond. Zo zijn er meer voorbeelden waarbij security management doorslaggevend is of kan zijn bij onderzoek naar interne, maar ook externe criminaliteit.

Andersom kan de methodiek van fact finding worden gebruikt bij een risico- of dreigingsanalyse. Immers, ook daar is het van belang dat er bij het in kaart brengen van risico's en dreigingen goed wordt doorgevraagd.

CONCLUSIE

Voor het goed functioneren van een organisatie is het uitermate belangrijk dat maatregelen en techniek die samenhangen met security management goed met elkaar in balans zijn (medewerkers ervaren de maatregelen/techniek niet als te zware belemmeringen in de uitvoer van hun werkzaamheden). Mocht zich dan onverhoopt toch iets voordoen, dan is daarnaast het uitvoeren van een grondig en objectief feitenonderzoek van belang.
Goed security management vergroot dus de kans op succesvol onderzoek. ■

Piet van Gelder heeft een politie-, recherche- en fraudeonderzoekachtergrond en verzorgt o.a. trainingen fraude awareness, security awareness en onderzoeksvaardigheden. Bregje De Lannoy-Walenkamp is trainer schriftelijke communicatie. Samen hebben zij de training Fact Finding ontwikkeld. www.fact-finding.nl